

CLAIMS

What is claimed is:

- 5 1. A method for determining authentication and authorization of queries comprising the steps of:
 - a) receiving a query that comprises user identification data, said query including an unencrypted portion that includes unencrypted data and an encrypted portion, said encrypted portion comprising an encrypted buffer
 - 10 encrypted using a first encryption key and a request buffer, said encrypted buffer and said request buffer encrypted using a second encryption key;
 - b) determining said second encryption key using at least a portion of said unencrypted data;
 - c) decrypting at least a portion of said encrypted portion of said query
 - 15 using said second encryption key determined in step b);
 - d) decrypting said encrypted buffer using said first encryption key;
 - e) determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer; and
 - f) provided said user identification data matches said user identification
 - 20 data contained within said encrypted buffer, determining authorization using information contained within said encrypted buffer.

2. A method as recited in Claim 1 further comprising the step of:
 - g) transmitting said unencrypted request buffer to a site that provides the
- 25 desired service when said query is determined to be authentic and authorized.

3. A method as recited in Claim 2 further including the steps of:

h) receiving a response from said site that provides the desired service;

and

5 i) forwarding said response.

4. A method as recited in Claim 3 wherein step i) further includes the steps of:

i1) encrypting said response; and

10 i2) forwarding said response.

5. A method as recited in Claim 3 wherein an authentication failure occurs when said encryption in step c) fails.

15 6. A method as recited in Claim 1 wherein said second encryption key is determined using a hash of at least three elements.

7. A method as recited in Claim 6 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly 20 generated number and a third encryption key.

8. A method as recited in Claim 6 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and said first encryption key.

9. A computer system comprising:
 - a processor coupled to a bus;
 - a memory unit coupled to said bus and comprising instructions that when executed by said processor implement a method for determining authentication and authorization of queries comprising the steps of:
 - a) receiving a query that comprises user identification data, said query comprising an unencrypted portion that includes unencrypted data and an encrypted portion, said encrypted portion comprising an encrypted buffer encrypted using a first encryption key and a request buffer, said encrypted buffer and said request buffer encrypted using a second encryption key;
 - b) determining said second encryption key using at least a portion of said unencrypted data;
 - c) decrypting at least a portion of said encrypted portion of said query using said second encryption key determined in step b);
 - d) decrypting said encrypted buffer using said first encryption key;
 - e) determining authentication by comparing said user identification data to user identification data contained within said encrypted buffer; and
 - f) provided said user identification data matches said user identification data contained within said encrypted buffer, determining authorization using information contained within said encrypted buffer.
10. A computer system as recited in Claim 9 wherein said method further comprises the step of:

g) transmitting said unencrypted request buffer to a site that provides the desired service when said query is determined to be authentic and authorized.

11. A computer system as recited in Claim 10 wherein said method
5 further comprises the steps of:

h) receiving a response from said site that provides the desired service;
and
i) forwarding said response.

10 12. A computer system as recited in Claim 11 wherein step h) of said method further comprises the steps of:

i1) encrypting said response; and
i2) forwarding said response.

15 13. A computer system as recited in Claim 11 wherein step i) of said method further comprises the steps of:

i1) compressing said response;
i2) encrypting said response; and
i3) forwarding said response.

20

14. A computer system as recited in Claim 9 wherein said second encryption key is determined using a hash of at least three elements.

15. A computer system as recited in Claim 14 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and a third encryption key.

5 16. A computer system as recited in Claim 14 wherein said second encryption key is determined by a MD-5 hash of said user identification data, a randomly generated number and said first encryption key.

17. A method for providing transaction processing in which
10 authentication and authorization of queries from a palmtop computer are determined comprising:
a) receiving a query from a palmtop computer, said query comprising user identification data, said query comprising an unencrypted portion that includes user identification data input by a user into said palmtop computer and
15 a randomly generated number, said query also comprising an encrypted portion that includes unencrypted data and an encrypted portion, said encrypted portion comprising an encrypted buffer encrypted using a first encryption key and a request buffer, said encrypted buffer including user identification data and authorization data, said encrypted buffer and said request buffer encrypted
20 using a second encryption key;
b) determining said second encryption key by performing a hash using said user identification data input by said user and using said randomly generated number and using a third encryption key;
c) decrypting at least a portion of said encrypted portion of said query
25 using said second encryption key determined in step b);

d) decrypting said encrypted buffer using said first encryption key;
e) determining authentication by comparing said user identification data input by said user to said user identification data contained within said encrypted buffer; and

5 f) provided said user identification data input by said user matches said user identification data contained within said encrypted buffer, determining authorization using said authorization data.

18. A method as recited in Claim 17 further comprising the step of:

10 g) transmitting said unencrypted request buffer to a site that provides the desired service when said query is determined to be authentic and authorized.

19. The method of Claim 18 further comprising the steps of:

15 h) receiving a response from said site that provides the desired service; and
i) forwarding said response to said palmtop computer.

20. The method of Claim 17 wherein said hash in step b) is a MD-5 hash.

21. The method of Claim 17 wherein said first encryption key is identical to said third encryption key.